

PROTECTION OF USER PROCESS DATA IN A SECURE PLATFORM ARCHITECTURE

Abstract of the Disclosure

- 5 A computer system includes at least one processor and a memory. A secure platform is stored in the memory for controlling the processor and the memory. An operating system image is stored in the memory for controlling the processor and the memory, and operates on top of the secure platform. An end user application is stored in the memory for controlling the processor and the
- 10 memory, and operates on top of the operating system image. The secure platform is configured to provide a secure partition within the memory for storing secret data associated with and accessible by the end user application. The secure partition is inaccessible to the operating system and other tasks operating on top of the secure platform.